

NAVAL WAR COLLEGE
Newport, R.I.

Information Warfare, Organizing for Action

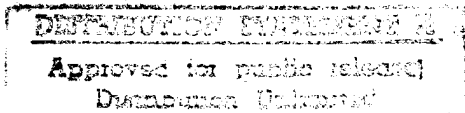
By

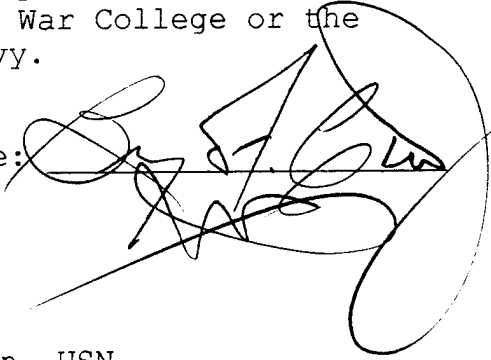
Benjamin F. Crew, Jr.

GG-14, Defense Intelligence Agency

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department.

The Contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.



Signature: 

20 May 1996

Paper directed by
Captain George W. Jackson, USN
Chairman, Joint Military Operations Department

DTIC QUALITY INSPECTED 4

Professor Roger Barnett
Faculty Advisor

Date

19960813 139

UNCLASSIFIED

Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): Information Warfare, Organizing for Action (Unclassified)			
9. Personal Authors: CREW, Benjamin F., Jr			
10. Type of Report: FINAL		11. Date of Report: 20 May 1996 14 JUN 1996	
12. Page Count: 31			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: information, information warfare, IW, Command and Control, Command and Control Warfare, C2W			
15. Abstract: The armed forces of the United States have recognized the potential importance of Information Warfare (IW) and have defined it as it will apply to military operations. It now remains for them to identify and implement an optimum organizational structure at the regional unified command level to develop, plan, synchronize and employ it effectively. Official publications recommend an "IW cell" made up members from the J3, J6 and J2 directorates of the CINCs staff. Any such organization needs unity of command, unity of effort and uniformity between the commands to succeed. Alternative organizational structures include a separate staff element, a single DoD Agency or service in charge, or a new functional unified combatant command--USINFOCOM. Although none of the organizations offers a solution that is totally acceptable, USINFOCOM may be the best alternative. That solution can only be implemented, however, after careful consideration of the way in which IW is to be viewed--as a force multiplier or as a form of warfare, and then only after today's warriors become aculturated to the phenomenon of IW.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841- 666 6461		20. Office Symbol: C	

Security Classification of This Page Unclassified

Abstract

Information Warfare, Organizing for Action

The armed forces of the United States have recognized the potential importance of Information Warfare (IW) and have defined it as it will apply to military operations. It now remains for them to identify and implement an optimum organizational structure at the regional unified command level to develop, plan, synchronize and employ it effectively. Official publications recommend an "IW cell" made up members from the J3, J6 and J2 directorates of the CINC's staff. Any such organization needs unity of command, unity of effort and uniformity between the commands to succeed. Alternative organizational structures include a separate staff element, a single DoD Agency or service in charge, or a new functional unified combatant command--USINFOCOM. Although none of the organizations offers a solution that is totally acceptable, USINFOCOM may be the best alternative. That solution can only be implemented, however, after careful consideration of the way in which IW is to be viewed--as a force multiplier or as a form of warfare, and then only after today's warriors become acculturated to the phenomenon of IW.

Table of Contents

I.	Abstract.....	ii
II.	Table of Contents.....	iii
III.	Acknowledgment.....	iv
IV.	Thesis.....	1
V.	Introduction.....	1
VI.	A Potential Problem.....	5
VII.	Information Warfare Today.....	6
VIII.	Historical Paradigms.....	9
IX.	Alternative Solutions.....	11
X.	Analysis.....	12
XI.	Unexpected Benefits.....	16
XII.	Conclusion.....	18
XIII.	Endnotes.....	20
XIV.	Bibliography.....	22

Acknowledgment

The author particularly wishes to acknowledge the contributions of Mr. Jeffrey Cooper of Science Applications International Corporation, whose observations and discussion served to focus the issues, and my Naval War College faculty advisor, Professor Roger Barnett, whose insight and encouragement stimulated the analysis. Without them, this paper would have been impossible.

Information Warfare: Actions taken to achieve information superiority by affecting adversary information, information based processes, information systems, and computer based networks, while defending one's own information, information based processes, information systems, and computer based networks.¹

CJCS Inst. 3210.01, 2 January 1996

Thesis

The Armed Forces of the United States have recognized the importance of information warfare and have arrived at an unclassified joint definition for this latest so-called "revolution in military affairs." It now remains for them to organize their assets to accomplish the actions suggested in that definition. A new functional combatant command--the United States Information Command (USINFCOM)--may offer the best solution in order to develop, plan, synchronize, and employ this unique new component of national power in armed conflict and in military operations other than war (MOOTW).

Introduction

In the aftermath of the 1991 Persian Gulf War, the Armed Forces of the United States recognized the important role played in that conflict by "Information Warfare" (IW), as described by Alan D. Campen in his book The First Information War. In the years since, a variety of books on the subject from philosophers like Alvin and Heidi Toffler (War and Anti-War) and storytellers like Winn Schwartau (Information Warfare: Chaos on the Electronic

Superhighway); numerous articles in military professional journals written by the likes of Gen. Gordon R. Sullivan and Adm. William A. Owens, Chief of Staff of the U.S. Army and Vice Chief of the Joint Chiefs of Staff respectively at the time they wrote, and a veritable plethora of unpublished War College student research papers, have examined the topic from almost every angle. The intent of these books, articles, and papers was first to firmly establish that the subject was indeed of enduring importance, and second to define it--to set boundaries on what should or should not be included in an understanding of the subject. These documents have been interspersed with directives, memoranda, and instructions from various Department of Defense (DoD) entities, promulgated to establish current policy on the subject. These have been periodically updated when deemed necessary. Some of the points of discussion that were raised have been resolved, others have not, and still others never will be resolved to the satisfaction of a majority of the participants. Readers interested in these issues, from whether "information warfare" was the appropriate title for the phenomenon, to whether IW is real or just a fad, and beyond, may refer to the expanded bibliography.

It is not the intent of this paper to re-visit those discussions, but rather to open debate on a facet of the issue that has been largely unaddressed to date--organization. To do

so, it is necessary to establish that IW is indeed recognized as important by the National Security and Defense establishments, that it has been clearly defined, and that the current definition has universal approval. These will provide a basis upon which to assess the existing organizational structure and perhaps to recommend changes should they seem advisable. To illustrate the importance of the subject, one need look no further than the National Defense University (NDU) in Washington D.C. which, in 1996, will graduate its second class from the School of Information Warfare and Strategy (SIWS), directed by Dr. John Alger. SIWS is the first new "senior service school" to be established in many years. Although SIWS will be absorbed into the National War College (NWC) curriculum² in the 1996-1997 academic year due a concern over the danger of "stove piping," the importance of the subject is undiminished. Future NWC students will be offered IW as an area of concentration.

As to definition, in addition to the definition of IW in CJCS Inst. 3210.01 quoted above, DoD Directive S-3600.1 states that IW comprises:

Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and information systems. (*Command and control warfare is a subset of information warfare.*) [*italics added.*]³

Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30 (CJCS MOP 30) further defines Command and Control Warfare

(C2W) as:

The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. [italics added]⁴

In addition to these "five pillars of C2W," CJCS MOP 30 also notes that; "Command and Control Warfare applies across the operational continuum and all levels of conflict" and that; "C2W is the military strategy that implements Information Warfare."⁵ Taken together, it is clear that IW includes the intangible (information and processes) and the tangible (systems and networks), that it has offensive and defensive components, that it is larger than simply the five aspects of C2W, and that it has an impact on every aspect of military operations from administration to civil affairs, including intelligence, communications, and logistics. Finally, Dr. Milan Vego of the U.S. Naval War College proffers a definition that reveals a glimpse into the affects of the various techniques:

...a series of actions conducted in support of national security strategy aimed to maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems. [italics added]⁶

One may surmise from all this that IW includes both the ability to acquire, protect, and move one's own information around the battlefield (Adm. Owens' "dominant battle space awareness") and

to destroy or render ineffective an adversary's information and information ~~acquisition~~, manipulation, and transmission equipment. How might the elements of these definitions affect the organization of assets to conduct IW?

A Potential Problem?

Is there indeed a problem? Is U.S. Information Warfare "broken?" Most importantly, are the Combatant Commanders in Chief (CINCs) able to conduct IW in the way they should, and are they well served by existing IW organizations? How are the combatant commands organized to conduct IW today, and are improvements being made? According to the Report of the Commission on the Roles and Missions of the Armed Forces (CORM):

...the U.S. Government,...lacks a comprehensive, integrated approach to the problems and opportunities raised by the explosive growth in reliance on information technology. In short, there is no overarching, government-wide concept for using IW to promote and protect U.S. national interests.⁷

This is a broad indictment, yet as a part of the commission's report, it clearly includes the Armed Forces. In addition, the CORM offered the following recommendations with respect to Command, Control, and Communications (C³) one of the targets of adversary IW: "(1) Better integrate C³ architectures and systems for CINC use. (2) Give the CINCs more peacetime control over theater communications resources."⁸

More specifically, according to Jeffrey Cooper, Director of Science Applications International Corporation's Center for

Information Strategy and Policy, there is little IW in the commands today. Conversely, much IW is imbedded in the service organizations; much that should be done by the CINC's! Even within the Commands, much of what is being done is being done by the components. For example, the Air Force's 14th IW Squadron is a part of U.S. Atlantic Command (USACOM).⁹

Perhaps most ominously, extremely limited IW assets that might be called upon by any regional CINC are widely dispersed both in space and administratively. Two trenchant examples are psychological operations units which are assigned to U.S. Special Operations Command (USSOCOM) in Florida, and the Joint C2W Center (JC2WC), "owned" by the Joint Staff in Washington, but located in Texas. There are, it seems, chinks in the armor! How can the situation be remedied? To understand how to get where one wants to go, it is best first to understand where one is.

Information Warfare Today

What are the recent paradigms? In 1993, Martin Libicki and James Hazlett wrote an article for the Joint Forces Quarterly entitled "Do We Need an Information Corps?" in which they offered a rationale and functions for such a corps. They clearly used for their model the recently formed "acquisition corps" of trained procurement officers. The article offered a cogent basis for such a corps and its functions, but left many implicit questions unanswered. This paradigm probably formed the basis

for the NDU SIWS course curriculum, but seems to have been rejected as ~~an~~ organizational model (given the absorption of the separate SIWS course into the NWC).

What then is the current state of regional combatant command IW organization? CJCS MOP 30 directed that the Combatant Commanders, "Designate a single staff component to be responsible for C2W..."¹⁰ and that the;

Chiefs of the Services and USCINCSOC, Designate a staff component to act as the single working level point of contact for C2W...require designation of staff components in subordinate commands...¹¹

These directions have been followed, but not exactly to the letter. Each command has found that no single staff element is capable of handling the full range of the command's IW requirements alone. For example, in the Joint Staff, there are IW divisions in both the J3 and J6 Directorates.¹² At the commands, in most cases, the result has been a "C2W" cell, made up of J3 and J6 staff officers (with the J3 representative serving as the senior member), usually with a J2 representative nearby. Some members of this "cell" are co-located (while others are not). CJCS Inst. 3210.01 notes that; "Many CINC C2W cells have integrated some disciplines (psyop, deception, etc.)..." but that; "Many disciplines have not been closely coupled in the past...cryptology, sophisticated jamming and counter-intelligence."¹³ The instruction further notes that most commands have C2W cells and that; "...integration of C2W into a

larger IW cell can facilitate deconfliction."¹⁴ All this complies with the advice offered by LtGen James R. Clapper, former Director of the Defense Intelligence Agency (an organization with no small stake in IW) that the J3 is the logical leader of a command's IW effort,¹⁵ and Jeffrey Cooper's admonition that "IW needs to be integrated into each of the regional Combatant Commands" and that "IW is more likely to be used regionally."¹⁶

One additional note is required. As Jeffrey Cooper further points out; "The organizational problem is complicated because each service is handling it [IW] differently."¹⁷ To illustrate, the Army's Land Information Warfare Center (LIWC) is subordinate to its Intelligence and Security Command. The Navy's Information Warfare Activity (NIWA) is subordinate to the Naval Security Group (also an intelligence organization), but its Director of IW and C2W is part of the staff of the Chief of Naval Operations subordinate to the Director of Space and Electronic Warfare (N6), and, in addition, the Navy also has its Fleet Information Warfare Center (FIWC), subordinate to USACOM, focused on support to the fleets. Finally, the Air Force has, in addition to the 14th IW Squadron mentioned earlier, its Information Warfare Center (AFIWC) which is subordinate to the Air Intelligence Agency.¹⁸ Curiously, each service obviously places heavy reliance on its intelligence infrastructure with respect to IW, but no one has

suggested that intelligence actually take the leading role. All of these service specific organizations have Title 10 "organize, train, and equip" implications, will serve their own service component commanders and personnel well, and should be retained. Yet in being so different from the existing operational paradigm they demonstrate yet again the inherent complexity of IW. This then is the conventional wisdom, but is it enough? Will it adequately support the CINCs? Will the incremental improvements directed by CJCS Inst. 3210.01 prove sufficient?

Historical Paradigms

Before attempting to identify and analyze alternative solutions to a potential problem, it may prove worthwhile to briefly examine the organizational development of the more mature military innovations of the 20th century--air forces, armored forces, and special operations forces. The first two began life as a "force multiplier" for the land army, and the third was a World War II child of necessity. Each had its pioneers, its philosophers, its proponents and detractors, and each grew into a unique organization fitted to its capabilities and characteristics, each became virtually a new type of warfare.

The first military airplanes were "scouts" used for visual reconnaissance as had cavalry before them. These were attacked by "pursuit planes" and the innovations grew to fighters and bombers. After World War I, visionaries like Douhet and Mitchell

advocated that the "Air Force" become a separate service, and by 1948 in the ~~United~~ States, it became a reality.

The first "tanks," a British name meant to disguise their true purpose, were intended to support the infantry in frontal assaults on enemy fortifications. Between the wars, future commanders like Guderian, Rommel, Patton, and DeGaulle advocated their use as weapons of maneuver and breakthrough. The Germans, of course, adopted these ideas and, most notably, the French did not, with the result that their tanks, which were in some ways superior to many of the German vehicles were decisively defeated. Today, armor remains a branch of the army, but the armored fist is considered by many to be the army's "arm of decision." Yet, since turnabout is fair play, tanks are routinely supported today by armored fighting vehicle mounted infantry.

Finally, modern Special Operations Forces were developed largely because the Western allies had no land army on the continent of Europe and had no other way to bolster the morale of the conquered peoples and annoy the Germans and their allies. These forces routinely operated independently (a "stove pipe"), and as their numbers grew as a result of their early successes, were employed in major operations, and suffered several tragic defeats (for example, the virtual destruction of the U.S. 1st Ranger Battalion "Darby's Rangers," and the combined U.S.-Canadian 1st Special Service Force "The Devil's Brigade".)

Following the war, such forces continued to be developed separately by each of the services (Special Forces, SEALs, Air Commandos) and were generally employed or assigned to operations by the services. It was not until after the Iran Hostage Rescue debacle that first the Joint Special Operations Command and subsequently USSOCOM were formed to ensure that limited resources were well coordinated and appropriately employed by the regional commands. Special operations remains in some ways, a "stove pipe," but through its Special Operations Component Commanders at the regional combatant commands, is today fully integrated into CINC planning and operations.

Alternative Solutions

All that has gone before suggests that there are two basic needs required of any IW organization at the operational (Combatant Commander/CINC) level of warfare. The first of these is **"unity of command,"** the necessity for all staff elements at a command to be aware of and involved in the planning and implementation of IW as an integral part of any operation. IW is, according to Mr. Cooper; "...not another purple door, but an 'operational' thing...and you don't want it to be thought of as something else."¹⁹ The second need is for **"unity of effort,"** which seeks an organizational solution that places scarce and often unique assets from each of the services in the hands of a single organization so that they can best be employed

synergistically. A third need, perhaps more desired than required, yet no less important for that distinction, is **uniformity**. Within the limits of the CINC's command prerogative, IW should function the same way in each regional area of responsibility (AOR), so as not to confuse the junior officers and enlisted personnel responsible for its implementation. This is, to a great degree, the task of doctrine, but precisely because IW doctrine is still immature, some uniformity now could only help in its development.

The existing organizational paradigm described above (the IW cell, composed of officers from various staff directorates) clearly satisfies the first requirement but does not seem to adequately address the other two. Are there alternatives? Yes! First, retaining the command focus, each command could establish a new and separate staff directorate for IW. Shifting to a national, or at least to a DoD-wide focus, other alternatives include assigning the responsibility for IW to a single DoD Agency or to a single service, and finally, forming a separate, functional, unified, Combatant Command, U.S. Information Command--USINFOCOM.

Analysis

How are we to determine if any of these solutions (including the existing structure) is significantly superior to the others? By examining each in relation to its ability to satisfy the three

stated needs. A basic decision matrix would prove over simplified in this case, however, because the scarcity of IW resources causes the two primary needs to be diametrically opposed. Therefore coincidental advantages and disadvantages also deserve consideration.

Considering each alternative in turn, the first (the IW cell) best satisfies the need for unity of command, offering synergy across the CINC's staff, however, with no assigned assets other than the selected staff officers (who may or may not be trained or qualified in IW), it fails to adequately address unity of effort, and offers no guarantee of command uniformity. It does offer the cheapest alternative (a non-trivial matter in the era of downsizing) since the cell members will likely be assigned "out of hide" from their original staff directorates, but given human nature, they might well be the members their bosses can "most afford to lose," and would likely only work on IW "part time." The second alternative (a separate J code) retains some intra-staff synergy, but, because IW would be in its own directorate, the other directorates might feel free to forget about it. A separate J code would likely be nearly as inexpensive as an IW cell (as long as no additional billets were requested) but the other directorates would be proportionally weakened by the reduction in their manning. Once again, it is unlikely that there would be additional IW assets assigned,

ensuring no better unity of effort than the existing structure and no more ~~uniformity~~ between commands.

Turning to the DoD-wide/less command focused alternatives, what DoD Agency might fulfill a role in overall charge of military IW? Two candidates are the National Security Agency (NSA) and the Defense Information Systems Agency (DISA), who, even today, compete for the communications security role (the CIA is not considered here because it is not a part of the armed forces). Both NSA and DISA have the experience, knowledge, and assets to handle at least the computer and security aspects of the task. NSA has, perhaps, more computer experience than any government agency.²⁰ Unfortunately, neither agency has combat operations credibility (although both clearly provide excellent support). Further, NSA lacks public credibility in the wake of the "clipper chip" encryption device controversy, according to a knowledgeable government source who has requested anonymity. Finally, even if funded to a level sufficient to accomplish the task at an acceptable level of unity of effort, with DoD-wide uniformity, neither agency could even remotely satisfy the unity of command need. What about a single service? According to Jeffrey Cooper, such an assignment would be politically unacceptable,²¹ but could it work? Perhaps. The service that is apparently most attuned to and prepared for IW is the Air Force. It already acquires and controls many of the systems that provide

much of the U.S. space borne information capability through Air Force Space ~~Command~~ and U.S. Space Command. Yet, according to the Air Force, the;

Air Force does not lay claim to IW. Rather it needs a national focus. Execution of IW objectives needs theater focus and orchestration, and should be done by service components as directed by the CINCs.²²

Not only does the Air Force demur, but difficulties would likely be encountered in joint assignments and other administrative details. However, should political realities and the service's willingness to accept the task change, the option might become viable. If so, the Air Force could satisfy IW's need for unity of effort (and offer a degree of uniformity) but would have major hurdles to overcome to achieve unity of command.

Finally, what of a functional unified command? Establishing such a command would certainly be the most difficult, complex, and costly solution to the IW dilemma, although it would most definitely satisfy the needs for both the unity of effort and uniformity. What of unity of command? Just as the regional CINCs, in concert with USSOCOM, have established special operations component commanders to achieve greater synergy in planing for special operations support, so too could IW component commanders be assigned in concert with USINFOCOM to achieve a similar level of planning for IW. Such component commanders would probably be senior to or equal in rank to the CINC's staff directors and likewise in a position, as a "commander," to

proselytize for IW. Perhaps not ideal, but the first solution that offers a chance to achieve all three command organizational IW needs. In contrast, Jeffrey Cooper offers several sobering thoughts. He does not favor an INFOCOM and asserts that "most CINCs" would agree with him. Cooper believes that; "If you stand up an information command, it becomes their business and everyone else walks away from it. A similar problem was experienced by U.S. Space Command (USSPACECOM)."²³ Likewise; "At the CINC level, IW is a much closer part of the operational plan than special operations."²⁴ This may be true, but it does not necessarily demonstrate that such problems cannot be overcome. Are there any other factors?

Unexpected Benefits

Suppose that USINFOCOM were established? What forces would be assigned to the various component commanders? Where would they come from? What impact might such transfers have on existing commands? These are questions that could easily serve as the basis for another detailed research paper, but they deserve to be mentioned here because of their potential affect on IW. For the sake of discussion, PSYOP units could be transferred from SOCOM to INFOCOM. The JC2WC could become a part of the INFOCOM staff (or part of the air component). The world-wide target data bases (target data sets are information) could be assigned to INFOCOM (air component) from the air component of

U.S. Strategic Command (STRATCOM), and satellite operations from the ~~components~~ of SPACECOM (weather, space tracking, and communications are also information). INFOCOM could even be assigned the operations of intelligence gathering aircraft and spacecraft (intelligence is certainly information). In theory, strategic nuclear weapons platforms and the defense of North America could be assigned to regional CINCs, and STRATCOM, SPACECOM, and much of the intelligence management infrastructure could be disbanded! All of these are topics with the potential for great controversy, but they deserve to be considered, not rejected out of hand. According to the Naval War College's Professor Roger Barnett; "The bloodiest battles in the Pentagon are fought over organizational issues," and arguments may well be based on the "not invented here" syndrome.²⁵

What about combat hardware? Attack and electronic warfare aircraft, information gathering naval vessels (submarines and Aegis equipped surface combatants), and information gathering ground forces would remain with their various components within the commands, but could be assigned tasks recommended by the information component commander as part of the operations plan. Once again, Jeffrey Cooper offers some cogent cautionary thoughts;

"You are dealing with multi-purpose forces with other missions. There may be a problem with doing structural damage to existing commands or organizations. If you don't pull out the right organizational pieces, you create a

command that doesn't have all the tools it needs.²⁶
Is it better ~~to~~ have a command that may be missing a few tools from its toolbox, or to have all the tools so widely separated that no one can ever use them all?

Conclusion

It appears that the results of the analysis of alternative organizational paradigms for Information Warfare at the operational level of war are less than thoroughly conclusive. No single solution seems to adequately and easily satisfy all of the stated organizational requirements. While it seems apparent that additional organizational maturation is needed to ensure optimum combatant command performance in IW, the current structure also seems appropriate, at least for the immediate future, to ensure the aculturation of warriors to the growing role of IW in modern military operations.

In the final analysis, the ultimate decision may rest on whether IW is viewed primarily as a force multiplier or as a type of warfare in its own right. It seems equally clear that although IW contains elements of both, one will dominate the other, at least for a time. The dominant factor may even change over time, perhaps more than once. The current institutional wisdom seems to argue for IW as a force multiplier. This view focuses on the ability to acquire, move, and use our own information, and to deny that ability to the enemy, which is the

more clearly understood side of IW. Yet if IW follows, even roughly, the ~~historical~~ pattern set by aviation, armor, and special operations, in a year, or in a decade, it will become, in the final analysis, a distinct form of warfare. The ability to forcibly penetrate an adversary's information systems and destroy or manipulate his data, the newer and less understood side of IW, will come to the forefront. IW, by its very nature, is more like special operations than armor or aviation. The similarities exist: joint but limited, service specific, multi-functional assets, specialized equipment, and unique personnel skills and training requirements. It therefore seems that ultimately, a functional unified command--USINFOCOM--always operating in a "supporting command" role like its sisters USSOCOM and U.S. Transportation Command (USTRANSCOM), offers the best chance for successful prosecution of information warfare operations in concert with more conventional efforts, and will become the IW organization of the future. One might hope that this organizational paradigm transition will be achieved without a costly failure such as that seen at Desert One.

The purpose of this paper is, once again, to stimulate thought and discussion. One hopes that it will result in the formulation of the "right" IW organization for the Armed Forces of the United States of America, or at the very least, in a step or two in that direction.

Endnotes

1. U.S. Dept. of Defense; Chairman, Joint Chiefs of Staff Instruction 3210.01: Joint Information Warfare Policy, (Washington: 1996), 6.
2. Interview with Dr. John Alger, Director, School of Information Warfare and Strategy, National Defense University, Washington, D.C.: 20 April 1996.
3. U.S. Dept. of Defense; Department of Defense Directive S-3600.1: Information Warfare, (Washington: Undated draft), 1.g
4. U.S. Dept. of Defense. Chairman, Joint Chiefs of Staff Memorandum of Policy No. 30: Command and Control Warfare, (Washington: 1993), 2.
5. Ibid., 2,3.
6. Milan N. Vego, "Operational Leadership" Unpublished Paper, U.S. Naval War College, Newport, RI: July 1995, 11.
7. Commission on the Roles and Missions of the Armed Forces, Directions for Defense, (Washington: 1995), 2-15.
8. Ibid., 2-5.
9. Interview with Jeffrey R. Cooper, Director, Center for Information Strategy and Policy, Science Applications International Corporation of McLean, VA, Newport, RI: 24 April 1996.
10. CJCS MOP 30, 19.
11. Ibid., 23.
12. Science Applications International Corporation, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, (Arlington VA: 1995), A-14.
13. CJCS Inst. 3210.01, B-1.
14. Ibid., B-5.
15. James R. Clapper, and Eben H. Trevino, Jr. "Critical Security Dominates Information Warfare Moves," Signal, March 1995, 71-72.
16. Cooper, interview.

17. Ibid.
18. Science Applications International Corporation, Information Warfare, A-18, A-24, A-25, A-30.
19. Cooper, interview.
20. James Bamford, The Puzzle Palace, Boston: Houghton Mifflin Company, 1982, 97-102.
21. Cooper, interview.
22. Science Applications International Corporation, Information Warfare, A-32.
23. Cooper, interview.
24. Ibid.
25. Interview with Professor Roger Barnett, U.S. Naval War College, Newport, RI: 24 April 1996.
26. Cooper, interview.

Bibliography

This ~~expanded~~ bibliography, while not encyclopedic, is offered to the interested reader both to stir interest and to illustrate the complexity and range of opinion on the subject of Information Warfare. The author offers the benefit of this research to those seeking to expand the body of knowledge of the topic. Some documents offer great quantities of information in copious detail, others offer short but pithy tidbits. All proved useful in some way. Much that was of interest was omitted from the paper due to length restrictions.

Arquilla, John. and David Ronfeldt. "Cyberwar Is Coming!"
Comparative Strategy, April-June 1993, 141-165.

Interview with Dr. John Alger, Director, School of Information Warfare Strategy, National Defense University, Washington, D.C.: 20 April 1996.

Bamford, James. The Puzzle Palace. Boston: Houghton Mifflin Company, 1982.

Beichman, Arnold. "Revolution in the Warfare Trenches."
Washington Times, 31 January 1996, 17.

Bowman, Tom and Scott Shane. "Battling High Tech Warriors; New Targets: National Security Agency Spies Target Computer Terrorism, Economic Espionage and Nuclear Weapons." The Baltimore Sun, 15 December, 1995, 1A.

Campen, Alan D. The First Information War. Fairfax, VA: AFCEA International Press, 1992.

_____. "Information Warfare is Rife With Promise, Peril."
Signal, November 1993, 19-20.

Clapper, James R. and Eben H. Trevino, Jr. "Critical Security Dominates Information Warfare Moves." Signal, March 1995, 71-72.

Commission on the Roles and Missions of the Armed Forces.
Directions for Defense. Washington: 1995.

Cooper, Jeffrey R. "Another View of Information Warfare: Conflict in the Information Age." Publication Draft, Science Applications International Corporation, 1995.

Interview with Jeffrey R. Cooper, Director, Center for

Information Strategy and Policy, Science Applications
International Corporation, McLean, VA: 25 April 1996.

Cothron, Tony L. "Achieving the Revolutionary Potential of
Information Technology." Unpublished Research Paper, U.S.
Naval War College, Newport, RI: 1995.

Devlin, Daniel D. "Psychological Operations." Lecture. U.S. Naval
War College, Newport, RI: 13 December, 1995.

DiNardo, R. L. and Daniel J. Hughes. "Some Cautionary Thoughts on
Information Warfare." Air power Journal, Winter 1995, 69-79.

Fogleman, Ronald R. "Information Operations: The Fifth Dimension
of Warfare." Defense Issues, vol. 10, no. 47, 1-3.

_____. "Fundamentals of Information Warfare - An Airman's
View." An Address to the National Security Industry
Association-National Defense University Foundation
Conference on the Global Information Explosion, Washington,
16 May 1995.

Folly, Frank E. "The Joint C2W Center." Lecture. U.S. Naval War
College, Newport, RI: 3 January, 1996.

Gravell, William. "Information Warfare, The Joint Staff
Perspective." Lecture. U.S. Naval War College, Newport,
RI: 31 January, 1996.

Grier, Peter. "Information Warfare." Air Force Magazine, March
1995, 34-37.

Harley, Jeffrey Allan. "The Role of Information Warfare: Truth
and Myths." Unpublished Research Paper, U.S. Naval War
College, Newport, RI: 1996.

Hasslinger, Karl M. "Information Warfare: What Is the Threat?"
Unpublished Research Paper, U.S. Naval War College, Newport,
RI: 1995.

Isensee, Ernst K. "Impacts on the Operational Commander in the
Information Age." Unpublished Research Paper, U.S. Naval War
College, Newport, RI: 1995.

Jensen, Owen E. "Information Warfare: Principles of Third Wave
War." Air power Journal, Winter 1994, 35-43.

Jones, Jeffrey B., and Michael P. Mathews. "PSYOP and the

Warfighting CINC." Joint Force Quarterly, Summer 1995, 28-33.

Killam, Timothy B. "Weapons of Mass Disruption for the Operational Info-warrior." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

Kraus, George F. "Information Warfare in 2015." U.S. Naval Institute Proceedings, August 1995, 42-45.

Krepinevich, Andrew F. Missed Opportunities: An Assessment of the Roles & Missions Commission Report. Washington: Defense Budget Project, 1995.

Libicki, Martin C. "What Is Information Warfare?" Strategic Forum, no. 28, May 1995, 1-4.

_____. "What Is Information Warfare?" Draft Version. Advanced Command Concepts and Technology Institute for National Strategic Studies, National Defense University, 21 July 1995.

_____. and James A. Hazlett. "Do We Need an Information Corps?" Joint Force Quarterly, Autumn 1993, 88-97.

Locke, Jeffrey S. "Command and Control Warfare: Promise and Challenge for the Operational Commander." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Markoff John. "Secure Digital Transactions Just Got Less Secure." The New York Times, 11 December 1995, A1, D6.

_____. "Plan to Guard Credit safety On Internet." The New York Times. 1 February 1996, D1, D7.

Marr, Patrick M. "Information Warfare and the Operational Art." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Miller, Charles E. "Net Assessments." Lecture. U.S. Naval War College, Newport, RI: 17 January, 1996.

Morris, Chris, Janet Morris, and Thomas Baines. "Weapons of Mass Protection." Air power Journal, Spring, 1995.

Munro, Neil, "The Pentagon's New Nightmare: An Electronic Pearl Harbor." The Washington Post, 16 July 1995, C03.

- Owens, William A. "The Emerging System of Systems." Naval Institute Proceedings, May, 1995.
- Ricks, Thomas E. "Warning Shot: How Wars Are Fought Will Change Radically, Pentagon Planner Says," The Wall Street Journal, 15 July 1995, A1, A5.
- Ross, Jimmy D. "Winning the Information War." Army, February 1994, 26-32.
- Round, W. Oscar, and Earle L. Rudolph, Jr. "Civil Defense in the Information Age." Strategic Forum Number 46. Washington: National Defense University, September 1995.
- Rowe, Wayne J. Information Warfare: A Primer for Navy Personnel. Strategic Research Department Research Report 6-95. Newport RI: U.S. Naval War College. Center for Naval Warfare Studies. Strategic Research Department, 1995.
- Rowell, Michael O. "Animal Crackers: Weakness in our C4I Strengths." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.
- Ryan, Donald E. "Implications of Information Based Warfare." Joint Force Quarterly, Autumn/Winter 1994-95, 114-116.
- Ryan, Julie, and Gary Federici. Offensive Information Warfare--A Concept Exploration. Alexandria, VA: Center for Naval Analysis, 1994.
- Ryan, Julie, Gary Federici, and Tom Thorley. Information Support to Military Operations in the Year 2000 and Beyond: Security Implications. Alexandria, VA: Center for Naval Analysis, 1993.
- Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.
- Science Applications International Corporation. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Arlington VA: 1995.
- _____. Planning Considerations for Defensive Information Warfare: Information Assurance. Arlington VA: 1993.
- Sexton, Joanne. "A Combatant Commander's Organizational View of Information Warfare and Command and Control Warfare." Unpublished Research Paper, U.S. Naval War College, Newport,

RI: 1995.

"Spy Wars: The Gulf War Flu." U.S. News and World Report, January 30, 1992, 50.

Stewart, John F. "Command and Control Warfare and Intelligence on the Future Digital Battlefield," Army Research, Development and Acquisition Bulletin, November-December 1994, 14-15.

Stein, George J. "Information Warfare." Air Power Journal, Spring, 1995.

Sullivan, Gordon R. and James M. Dubik. "War in the Information Age," Military Review, April 1994, 46-62.

Sun Tzu. The Art of War. Translated by Samuel B. Griffith. New York: Oxford University Press, 1963.

Swider, Gregory, Harry Schmalz, Richard Heaton, Lloyd Koenig, and Mein-Sieng Wei. Information Warfare/C2 Warfare: Summary Report. Alexandria, VA: Center for Naval Analysis, 1995.

Tempestilli, Mark. "Waging Information Warfare: Making the Connection Between Information and Power in a Transformed World." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Toffler, Alvin and Heidi Toffler. War and Anti-War. Boston: Little, Brown and Company, 1993.

U.S. Armed Forces Staff College. Joint Command and Control Warfare Staff Officer Course Student Text. Norfolk, VA: 1995.

U.S. Armed Forces Staff College. The Joint Staff Officer's Guide 1993. AFSC Pub 1. Norfolk, VA: 1993.

U.S. Dept. of Defense. Chairman, Joint Chiefs of Staff Instruction 3210.01: Joint Information Warfare Policy. Washington: 1996.

U.S. Dept. of Defense. Chairman, Joint Chiefs of Staff Memorandum of Policy No. 30: Command and Control Warfare. Washington: 1993.

U.S. Dept. of Defense. Directive S-3600.1: Information Warfare. Washington: Undated Draft.

U.S. Dept. of Defense. Joint Pub 0-2: Unified Action Armed Forces (UNAAF). Washington: 1995.

U.S. Dept. of Defense. Joint Pub 3-0: Doctrine for Joint Operations. Washington: 1995.

U.S. Dept. of Defense. Joint Pub 3-07: Joint Doctrine for Military Operations Other Than War. Washington: 1995.

U.S. Air Force. Cornerstones of Information Warfare. Washington: 1995

Vego, Milan N., "Operational Leadership." Unpublished Paper, U.S. Naval War College, Newport, RI: July 1995, 11.

Walters, Dan. "The Fleet Information Warfare Center." Lecture. U.S. Naval War College, Newport, RI: 7 February 1996.

Washington, Douglas Waller. "Cyber Soldiers," Time, 21 August 1995, 38-44.

Widnall, Sheila E., and Ronald R. Fogleman. "Global Presence." Joint Force Quarterly, Spring 1995, 94-99.